Australian Government

National Security Science and Technology Priorities

2020

NATIONAL SECURITY SCIENCE AND TECHNOLOGY PRIORITIES

We live in an environment of great technological change. The scope of science and technology is broadening and the speed of change is unprecedented. This has a particular impact on Australia's national security capability and as such, presents us with both challenge and great opportunity. The manner in which Australia responds to this paradigm shift has potential to shape our sovereign standing.

Given the commitment and capacity of adversaries to engineer smarter, more agile and increasingly innovative technologies to threaten our national security, and the growing challenges arising from our natural environment that test the resilience of our society and national systems, Australia needs to remain at the forefront of science and technology in order to remain agile and anticipative of new and emerging threats. The time available to detect and react to technological developments is decreasing, and in doing so creating the potential to diminish our institutional responsiveness.

The National Security Science and Technology Priorities seek to drive a strategic advantage by clearly articulating the national security community science and technology challenges, therefore assisting to shape and influence programs of work across both the national security agencies and the broader science and technology ecosystem. In addition, they provide the science and industry community with visibility of the endorsed national security science and technology areas we seek alignment, partnership and activity.

The updated set of National Security Science and Technology Priorities have been developed by the National Security Science and Technology Centre with broad input, close engagement and agreement across the national security community, and will be reviewed regularly to ensure they remain current. The collaborative manner in which the community has developed a collective view of its science and technology challenges is notable and a symbol of strong alignment moving forward. These priorities provide a thorough update to the National Security Science and Technology Policy and Priorities which were released in May 2018, with greater consideration given to national and social resilience, and seek to encourage innovative thinking on how best to address Australia's national security challenges.

The National Security Science and Technology Centre within Defence Science and Technology coordinates whole-of-Government science and technology for national security. It strives to partner widely across the community in order to improve impact, encourage alignment and reduce duplication.

National Security Science and Technology Priorities

The six National Security science and technology priorities are described in more detail on the following pages, including their strategic drivers and specific science and technology challenges.

1. Technology Foresight (Page 3)

The ability to monitor, analyse and evaluate the implications of scientific and technological developments to prevent strategic and tactical surprise.

2. Intelligence (Page 6)

The ability to collect, analyse, integrate, assess and disseminate intelligence with the accuracy, scale and speed required to support timely national security and intelligence decision making.

3. Preparedness, Protection, Prevention & Incident Response (Page 11)

The ability to appropriately equip and prepare Australian agencies to effectively address national security threats and natural or man-made destructive events, including mass-harm and mass-damage incidents, either by preventing their occurrence, or responding and recovering effectively if they have occurred.

4. Cyber Security (Page 15)

The ability to strengthen the cyber security and resilience of critical infrastructure and systems of national significance through the conduct of research and development, and the delivery of advanced cyber technologies, tools, techniques and education.

5. Border Security and Identity Management (Page 18)

National security community's ability to protect and secure Australia's borders from disease outbreaks, hazardous material and threats to our community, including maximum disruption effect on illegal activity and migration with projected growth in people and cargo movement across Australian borders.

6. Investigative Support and Forensic Science (Page 22)

Law enforcement's ability to prevent, disrupt and prosecute terrorist and criminal activities in a complex transnational and evolving digital environment.

Key Contact

Dr Richard Davis
Chief Technology Officer – National Security
richard.davis@dst.defence.gov.au
(02) 6128 6590

General Enquiries

nsstcexternal@dst.defence.gov.au

TECHNOLOGY FORESIGHT

CHALLENGE

The ability to monitor, analyse and evaluate the implications of scientific and technological developments to prevent strategic and tactical surprise.

Enhancing technology foresight in Australia

The ability to monitor, detect and model new game changing technologies.

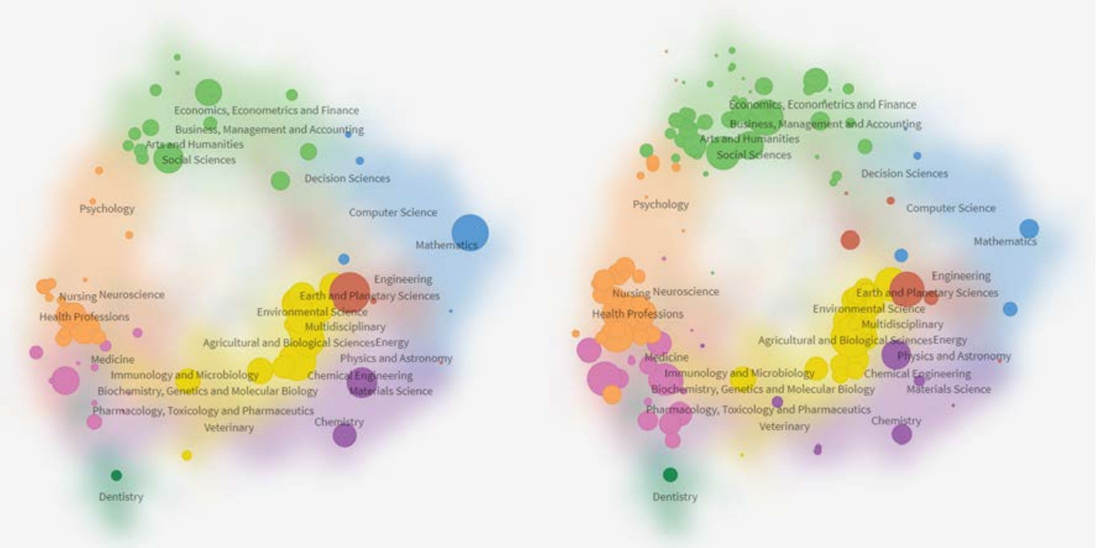
Advancing methods in data analytics

The ability to detect trends in large quantities of mixed-source unstructured data.

Strategic Drivers

Research and development of technology has increased rapidly over the past 40 years facilitated by complex interactions between financial investment, human capital, flow of knowledge, security threat perceptions and government funding of major research facilities. Moreover, society's dependence on technology has significantly increased over the past two to three decades creating an ever growing desire for more technology, capable of performing more complex and diverse tasks more quickly.

This rapid rate of technological development has been facilitated by a range of factors including greater funding to university/research institutes; a growing population of a more highly educated and qualified workforce; and improved accessibility to research facilities. Coupled with the substantial growth in volume of research there have been changes in the distribution of research subjects, as indicated below for the Australian research and development landscape.



Distribution of research subjects in Australia (L to R: 2000; 2016) Larger bubbles represent a greater number of publications within a certain subject area.

This trend is expected to increase into the foreseeable future, driven by further investment, more sophisticated infrastructure supporting highly technical experiments, and larger numbers of people employed in the research and development sector.

Alongside greater sophistication to everyday technology is the diversification of its potential application and commercialisation. The rise of technology will see future technology-based hardware able to be bought 'off-the-shelf' and integrated into customised products to suit desired capability. In an age where the financial resources of some non-state actors exceed that of many nation states, the potential for illegal and extra-legal organisations to leverage technological advancement represents a significant threat. This threat extends beyond the advantages of purchasing power and into a variety of applications that cannot be matched or foreseen by nation states. The above also highlights the importance of critical technology security in preserving Australia's national interest.

The consequence of such a dynamic and complex environment makes it important that we strategically drive investments in those national security capabilities which provide Australia with the capacity to detect, assess and address threats early and avoid strategic surprise, and identify opportunities for building Australia's domestic sovereign capability in critical technologies.

Science and Technology Challenges

The technology foresight priority area is unique in that it is a capability in itself and enables excellence across the other five science and technology priority areas. The priorities for this area are therefore focused on enhancing the power and effectiveness of technology foresight itself.

1. Enhancing technology foresight in Australia

Technology foresight in Australia is an area of significant interest and growth for the community. Efforts across government are developing a cohesive approach to technology foresighting. Effective technology foresight depends on a good understanding of future environments and associated capability requirements, which the national security community can develop in order to leverage this capability to its benefit. The community must therefore be strong supporters and contributors to a whole of government technology foresight effort.

Examples of science and technology research include:

- Evolving and improving technology foresight techniques and methodologies; and
- Improving abilities to model complex social, political, economic, technological interactions.

2. Advancing artificial intelligence, machine learning and data science capabilities[1]

There is a role for the broader national security science and technology community in working together to leverage technology foresight for success. Data analytics is at the core of effective identification of emerging technology. The ever-increasing volume of technological advancement necessitates an analytics-driven approach based on artificial intelligence and machine learning. Advances in natural language processing, automated translation and intuitive searching algorithms have the capacity to significantly advance the technology foresight capability. There is also significant opportunity for academia to engage with a technology foresight capability through the provision and support of horizon scanning and foresight methodologies and training.

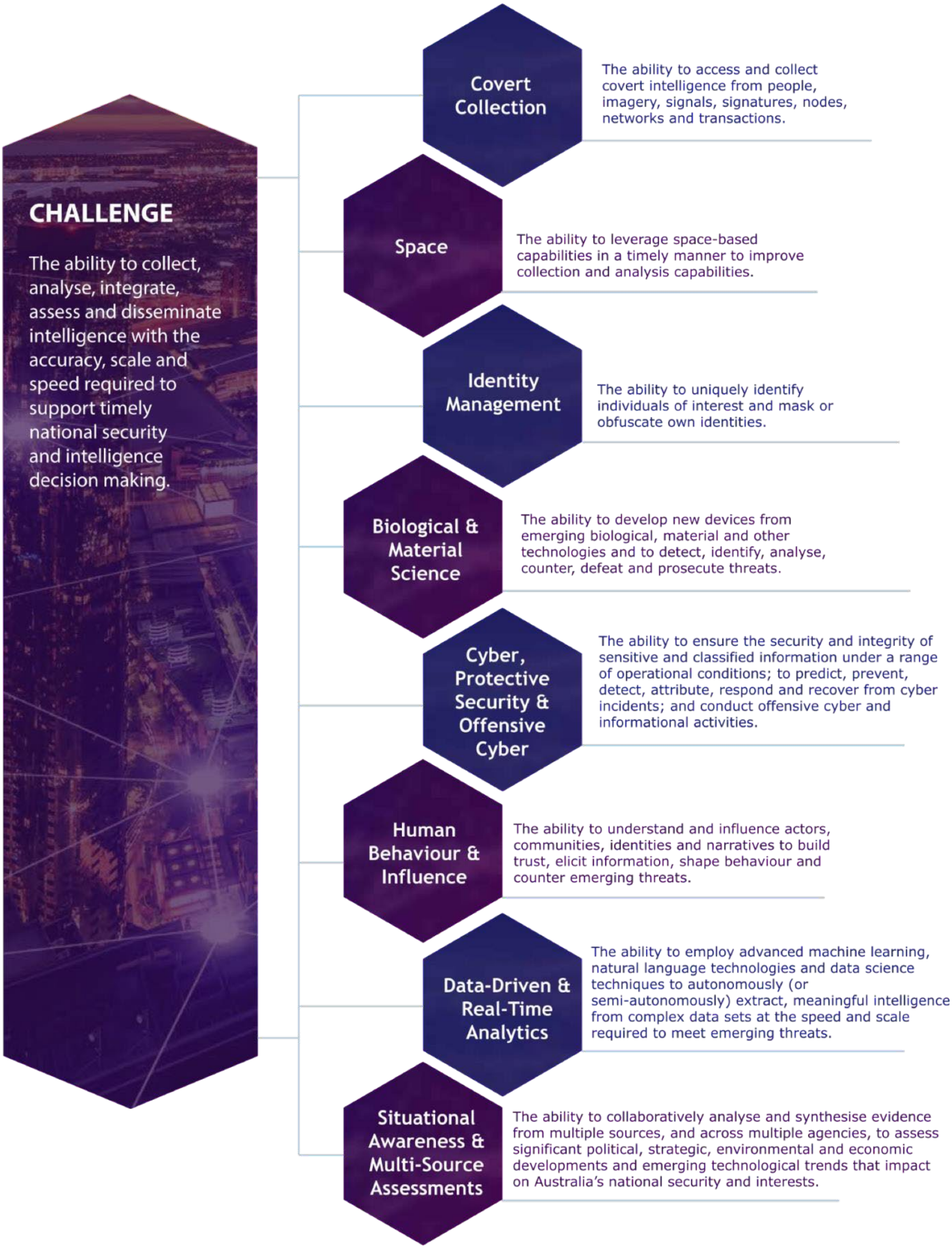
Most importantly, the power of technology foresight comes from access to big data; larger and more diverse data sets are required and will include sources such as intellectual property databases, venture capital data, domestic and international academic publications, as well as open source RSS feeds and the like. A concentrated effort to consolidate and provide access to these data sets will be critical in a successful technology foresight capability.

Examples of science and technology research include:

- Development of predictive algorithms for technology development
- Developing methods for detecting trends in social/corporate/academic based events
- Improving abilities to handle and process large amounts of mixed-source and complex unstructured data
- New methods for obtaining open-source data for analysis; and
- Improved techniques for visualising complex developments in technology or the interaction between various drivers.

1: Applies across all six NSST priorities

INTELLIGENCE



CHALLENGE

The ability to collect, analyse, integrate, assess and disseminate intelligence with the accuracy, scale and speed required to support timely national security and intelligence decision making.

Covert Collection

The ability to access and collect covert intelligence from people, imagery, signals, signatures, nodes, networks and transactions.

Space

The ability to leverage space-based capabilities in a timely manner to improve collection and analysis capabilities.

Identity Management

The ability to uniquely identify individuals of interest and mask or obfuscate own identities.

Biological & Material Science

The ability to develop new devices from emerging biological, material and other technologies and to detect, identify, analyse, counter, defeat and prosecute threats.

Cyber, Protective Security & Offensive Cyber

The ability to ensure the security and integrity of sensitive and classified information under a range of operational conditions; to predict, prevent, detect, attribute, respond and recover from cyber incidents; and conduct offensive cyber and informational activities.

Human Behaviour & Influence

The ability to understand and influence actors, communities, identities and narratives to build trust, elicit information, shape behaviour and counter emerging threats.

Data-Driven & Real-Time Analytics

The ability to employ advanced machine learning, natural language technologies and data science techniques to autonomously (or semi-autonomously) extract, meaningful intelligence from complex data sets at the speed and scale required to meet emerging threats.

Situational Awareness & Multi-Source Assessments

The ability to collaboratively analyse and synthesise evidence from multiple sources, and across multiple agencies, to assess significant political, strategic, environmental and economic developments and emerging technological trends that impact on Australia's national security and interests.

Strategic Drivers

The 2017 Independent Intelligence Review (IIR) identified a number of challenges facing Australia's intelligence enterprise over the coming decade. These included the increasing complexity of the geostrategic environment, broadening scope of national security and intelligence missions, rapid pace of scientific and technological change and high levels of innovation investment by other nations. To meet these challenges the Review recommended changes to the coordinating structures, funding mechanisms and legislative arrangements governing an expanded National Intelligence Community (NIC) as well as a more systematic approach to leveraging science and technology. The subsequent Office of National Intelligence (ONI) Act 2018 established ONI with the mandate to lead the NIC and, among other things, *"ensure a structured and appropriate response to technological advancements"*.

Science and Technology Challenges

Through a process of consultation and analysis, eight priority challenges were identified to be pursued for research and development.

1. Covert collection challenges

   The ability to access and collect intelligence from people, imagery, signals, signatures, nodes, networks (including internet-of-things environments) and transactions with a low probability of detection and/or attribution. The ability to defeat adversary collection and cyber capabilities to safely move people, information and equipment into, out of, and through environments with low signature and likelihood of detection and/or attribution.

   Examples of science and technology research include:

   - Access technologies
   - Imagery and geospatial intelligence
   - Sensors, signatures, signals and networks
   - Computer network exploitation
   - Covert, secure and assured communications
   - Financial intelligence; and
   - Cryptocurrency, block-chain and distributed ledger technologies.

2. Space-based challenges

   The ability to leverage low cost and innovative technological advancement in space-based and high-altitude capabilities in a timely manner to improve collection and analysis capabilities.

   Examples of science and technology research include:

   - Launch technologies
   - Mission control systems and systems integration
   - Satellite communications, sensors and networks
   - Automation and on-board processing and analysis
   - Advanced materials
   - Space-based situation awareness; and
   - Counter space-denial capabilities.

3. Identity management challenges

The ability to quickly, accurately and uniquely identify individuals from all types of data (online, surveillance, biometric, forensic, text, etc), including where the data has low linkages to real world identities. The ability to mask or obfuscate the identity of an individual from adversaries where access to online, surveillance, biometric, forensic or other data is available.

Examples of science and technology research include:

- Biometrics (including behavioural biometrics)
- Deepfakes and generative adversarial networks (GAN)
- Bio- and geo- forensics (including for law enforcement and prosecutions)
- DNA/RNA
- Web-scraping and machine learning for identity data
- Counter biometric surveillance; and
- Socio-technical systems and systems integration.

4. Emerging biological and material science exploitation challenges

The ability to develop methodologies, techniques, services and devices from emerging biological, material and other technologies to provide new or alternate options to meet existing and future intelligence mission objectives. The ability to detect, identify, analyse, counter, defeat and prosecute threats from emerging technologies, in a safe and timely manner. The ability to exploit advances in machine learning to enable the above.

Examples of science and technology research include:

- Biotech engineering (e.g. CRISPR)
- Synthetic biology (e.g. data storage)
- Immunology and microbiology (e.g. gene sequencing and applications)
- Nanotechnology and material science (e.g. miniaturisation and new functions)
- Convergence or integration of technologies (e.g. nano-, bio- and info- technologies)
- Human augmentation technologies, human-machine interface,wearable devices; and
- Threat detection and remediation (e.g. explosives, radiological and pathogens).

5. Cyber security, protective security and offensive cyber challenges

The ability to ensure the security and integrity of sensitive and classified information whilst enabling flexible/remote working and crisis response. The ability to predict, prevent, detect, attribute, respond and recover from cyber incidents and malign online interference (foreign, domestic, insider) at a national scale. The ability to conduct offensive cyber and informational activities to disrupt emerging security threats.

Examples of science and technology research include:

- Cyber (and national infrastructure) systems analysis, vulnerability, risk, resilience
- Human aspects of cyber security (e.g. insider threat, behavioural analysis)
- Mobile device trust/assurance for remote and collaborative working
- Secure data transport
- Networking and sensor technologies (including internet-of-things)

- Supply chain security/intelligence
- Cryptography, quantum technologies and photonics; and
- Automated at-scale response.

6. Human behaviour and influence challenges

The ability to identify and understand actors' psychologies, social identities, narratives and behaviours that constitute a threat to Australia's security. The ability to mitigate and counter cultural, psycho-social and organisational drivers and antecedents to national security threats. The ability to influence target audiences to elicit information, affect behaviour or shape preferences.

Examples of science and technology research include:

- Network analysis and disruption techniques (criminal, terrorist, etc)
- Analysing online behaviour and profiling individuals and groups
- Building trust, rapport and influence and eliciting information
- Identifying and countering malign interference, influence and disinformation
- Identifying drivers, antecedents and pathways to radicalisation and extremism
- Understanding actors, communities, cultures, identities and narratives and influencing effects/outcomes
- Identifying trends in transnational, serious and organised criminal activities; and
- Influencing 'crowd' or mass behaviour.

7. Data-driven and real-time analytical challenges

The ability to employ advanced machine learning, natural language technologies and data science techniques to autonomously (or semi-autonomously) identify, extract, fuse and disseminate meaningful intelligence from large, disparate, sparse and/or incomplete data sets, including linguistic (text, speech, etc), geospatial, financial, signals, identity and other relevant data sets. The ability to do this at the speed and scale required to meet emerging threats.

Examples of science and technology research include:

- Data management, data engineering and data curation
- Automated information fusion, filtering, triage and knowledge management
- Advanced sampling, pattern recognition, predictive analytics and statistics
- Natural language processing and other language technologies
- Deep learning for large and disparate data sets
- Human-systems integration and uncertainty analysis; and
- Ethical, legal and societal aspects of AI/ML (trust, bias, discrimination, privacy, etc).

8. Situation awareness and multi-source assessment challenges

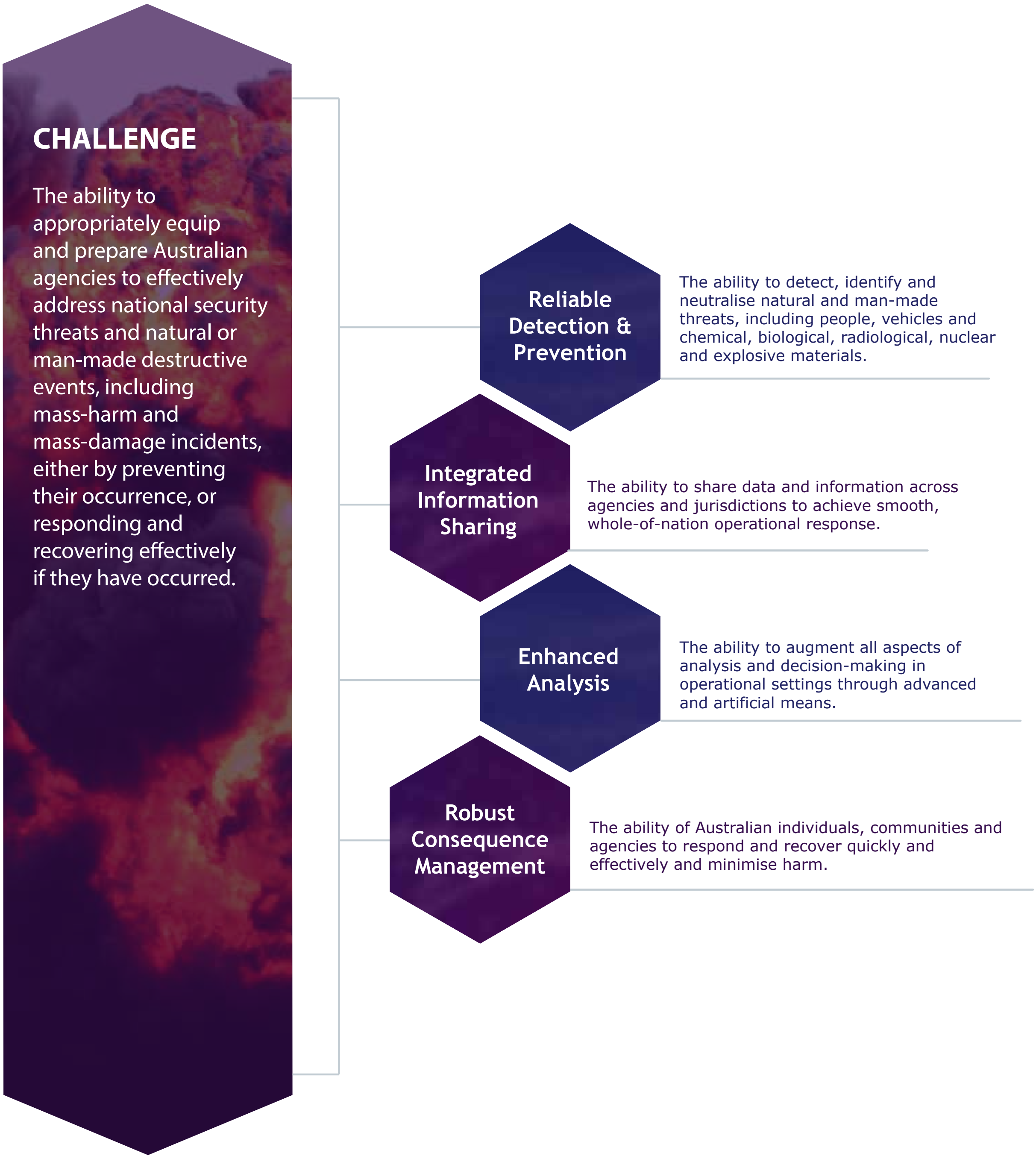
The ability to analyse and assess significant events and trends that impact on Australia's national security and interests (including political, strategic, environmental and economic developments as well as trends in adversarial behaviour, capability or investment in science and technology). The ability to collaboratively analyse and synthesise evidence from multiple sources, and across multiple agencies, to produce timely, high quality and influential intelligence reports and assessments. The ability to articulate the basis and level of confidence in assessments.

Examples of science and technology research include:

- All-source intelligence integration and collaboration technologies
- Political, strategic, economic and 'drivers of conflict' research and analysis
- Advance 'red-teaming', 'war-gaming', scenarios and course of action analysis
- Technology forecasting: emerging, critical and disruptive technologies
- Security implications of environmental change and health crises
- Risk and resilience frameworks and measurements for security threats
- Understanding and avoiding bias (e.g. algorithmic bias) and generating confidence measures for assessments; and
- Enhancing cognition, comprehension, learning and decision-making (e.g. visualisation, etc).

These priorities have been developed as a collaboration between the National Security Science and Technology Centre and the Office of National Intelligence (ONI), aided by a DST Science Counsellor embedded within ONI. They have been endorsed by the NIC Enterprise Management Committee and are designed to guide investment in science and research across the ten agencies of the NIC.

PREPAREDNESS, PROTECTION, PREVENTION AND INCIDENT RESPONSE



CHALLENGE

The ability to appropriately equip and prepare Australian agencies to effectively address national security threats and natural or man-made destructive events, including mass-harm and mass-damage incidents, either by preventing their occurrence, or responding and recovering effectively if they have occurred.

Reliable Detection & Prevention

The ability to detect, identify and neutralise natural and man-made threats, including people, vehicles and chemical, biological, radiological, nuclear and explosive materials.

Integrated Information Sharing

The ability to share data and information across agencies and jurisdictions to achieve smooth, whole-of-nation operational response.

Enhanced Analysis

The ability to augment all aspects of analysis and decision-making in operational settings through advanced and artificial means.

Robust Consequence Management

The ability of Australian individuals, communities and agencies to respond and recover quickly and effectively and minimise harm.

Strategic Drivers

The continual need for the movement of people, goods and ideas to maintain Australia's advanced economy and associated prosperity, carries with it the risk of introducing capabilities and human agents that are able to cause large-scale harmful events. Currently, Australia faces the prospect of persons or groups motivated to do harm to our citizens, infrastructure, economy and way-of-life. Novel methods and capabilities are continuously appearing, driven in part by advancing science and technologies. Consequently, Australia needs to keep abreast of these developments so that effective counter-measures can be generated and employed in a timely fashion. This is most effectively done if Australia is at the forefront of technological progress, undertaking the leading work that is keeping pace or ahead of these advances and exploiting these technologies earlier than anyone else. Therefore it is a priority to advance science and technology that improves the prevention of, containment of, response to, or recovery from, harmful mass-effect events. In addition, monitoring and enhancing national and social resilence (individuals and communities) is critical to successfully implement the right responses and recovery plans to adapt to rapid and crisis driven change (e.g. bushfires, floods, pandemics).

The specific drivers in this area include, inter alia:

- The appearance of novel compounds, components or agents or delivery mechanisms that are less detectable or more powerful when activated
- The advancements in remotely controlled and unmanned vehicles (UV) to be less detectable and more intelligent, more complex, carry better sensors and deliver more powerful payloads
- The constant vulnerability of fixed locations and infrastructure to attack, especially from remotely controlled or UV
- The ability of multiple and cross-jurisdictional agencies to respond to events in a sufficiently efficiently and effectively coordinated manner
- The challenges inherent in rapidly identifying potential threats in complex environments, be they physical or digital
- The ability of individuals, communities, government agencies, critical infrastructure and systems to be resilient and recover from incidents quickly; and
- The advancements in AI and ML to both enhance and degrade the protection of people and places.

Science and Technology Challenges

Through a process of consultation and analysis, four priority challenges were identified to be pursued for research and development.

1. Reliable detection and prevention

   Rapid and reliable detection of potential threats is an important enabler to preventing mass-harm and mass-damage events. There are two basic dimensions to this problem: the harmful agent and the delivery mechanism. Consequently it is continually important to be able to detect Chemical-Biological-Radiological-Nuclear-Explosive (CBRNE) compounds and weapons that are concealed. In addition, the speedy identification of people, luggage/freight and vehicles remains a priority concern. Remotely controlled and unmanned vehicles, particularly the airborne type, pose a heightened threat in their ability to evade detection and tracking and resist neutralisation. It is important to develop remote, stand-off and portable systems as this increases the safety of people, potentially decreases the damage to infrastructure and improves the flow of people and goods through areas. This also includes the monitoring of natural disasters and severe disease outbreak as they evolve to enable better situational awareness for responders and the public.

Examples of science and technology research include:

- Conduct remote, stand-off, non-invasive and portable sensing
- Conduct rapid and reliable CBRNE detection
- Countering/suppression of threat device remote initiation systems
- Means for the mass communication of incident and emergency information in crowded places (eg. stadiums)
- Identify individuals and vehicles in complex environments
- Detect and track small UV; and
- Remotely disable/control UV.

2. Enhanced analysis

The ability to conduct vulnerability assessments is a key precursor to the development of threat mitigation and prevention strategies. Likewise, the ability to model threat consequences (eg. casualties, infrastructure damage) is key to the planning of emergency response management and business recovery planning.

Through the application of AI, ML and Data Science (DS) algorithms, there is potential for enhanced detection, identification, tracking, situational awareness, analytics and decision support in the full gamut of operational scenarios. Advanced analytics should support the exploitation of social media and internet data to provide earlier detection and improved influence of potential threats in the cyber and social domains.

Examples of science and technology research include:

- Assessment and development of vulnerability modelling tools to identify and prioritise risks and the development of mitigation options
- Use of event consequence modelling to plan emergency response requirements
- Conduct AI/ML/DS-enhanced detection, identification and tracking
- Conduct AI/ML/DS-enhanced situational awareness, analytics and decision-support
- Exploit social media and internet data; and
- Perform advanced analysis of extremism in social groups.

3. Robust consequence management

Research into the neutralisation of CBRNE compounds and the after-effects of delivery improves the remediation of contaminated locations. Advanced analysis, modelling and simulation of mass-harm and mass-damage events or crisis, both natural disasters (including severe disease outbreak) and man-made, improves the design of structures and the planning of response actions. The safety and security of first responders in hazardous situations needs to be maximised through the use of appropriate physical protection and the use of remote-controlled and robotic systems. Investigation of what enables resilient individuals, societies and infrastructure is of key concern.

Examples of science and technology research include:

- Detect and remediate CBRNE events
- Model the evolution and impact of CBRNE events
- Protect first responders through knowledge of threat properties, safe handling, neutralisation procedures and personal protective equipment
- Utilise robotics and remote-controlled systems in hazardous environments; and
- Shape resilient people, communities, critical infrastructure and systems.

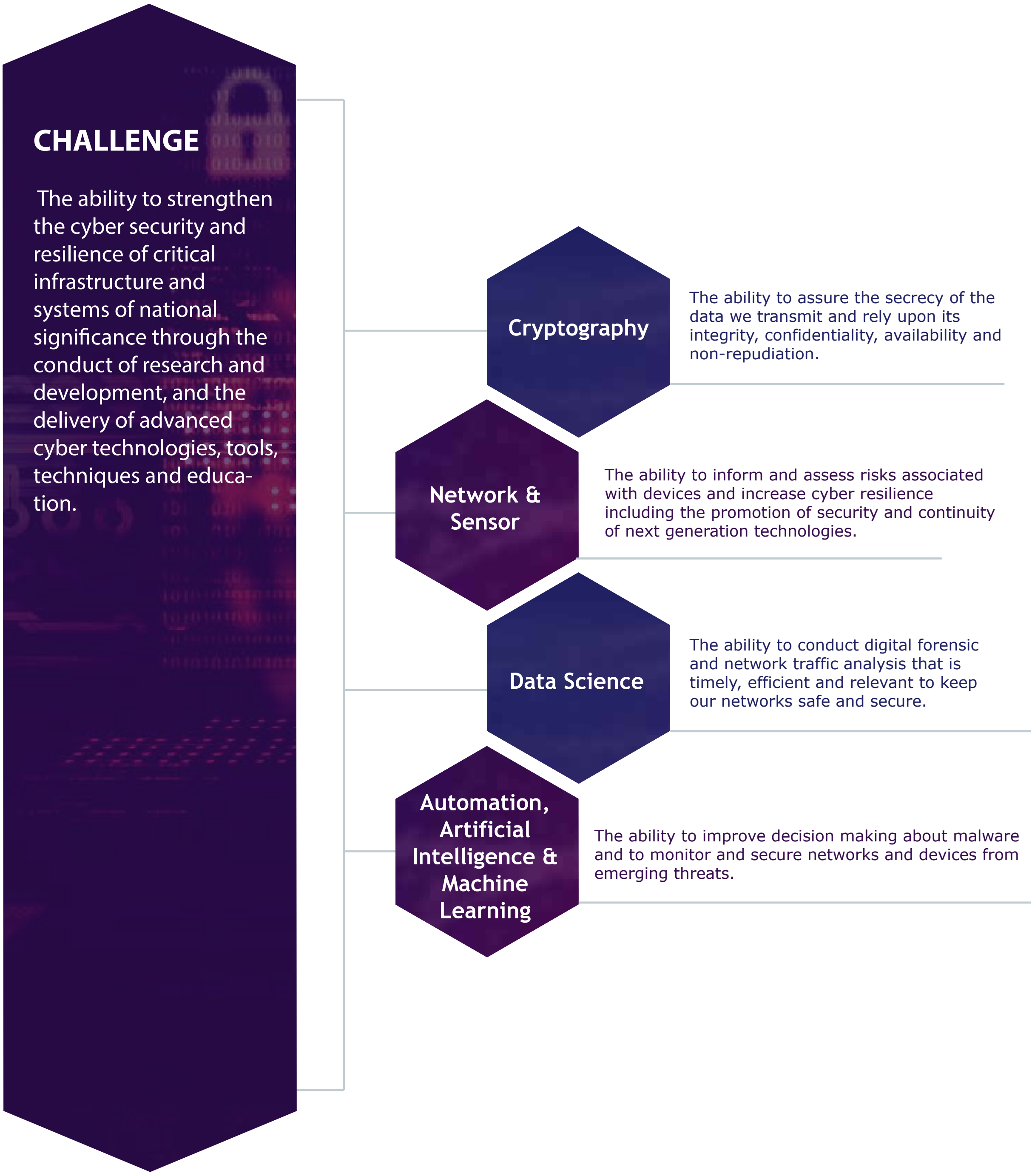
4. Integrated information sharing

Improving the ability of individuals and teams from different organisations and agencies to communicate and share data would greatly enhance the multi-agency and cross-jurisdictional response to mass-effect events. More coherent and comprehensive integration of communications systems and computers, so that data and information can be shared and fused speedily and accurately, would enhance the timeliness and effectiveness of these response efforts. Modelling and analysing multi-agency exercises and operations is vital to improving their design and planning.

Examples of science and technology research include:

- Achieve smooth multi-agency Command, Control and Communications
- Integrated and interoperable communications and information systems; and
- Integrated sharing, management and fusion of data and information.

CYBER SECURITY



CHALLENGE

The ability to strengthen the cyber security and resilience of critical infrastructure and systems of national significance through the conduct of research and development, and the delivery of advanced cyber technologies, tools, techniques and education.

Cryptography

The ability to assure the secrecy of the data we transmit and rely upon its integrity, confidentiality, availability and non-repudiation.

Network & Sensor

The ability to inform and assess risks associated with devices and increase cyber resilience including the promotion of security and continuity of next generation technologies.

Data Science

The ability to conduct digital forensic and network traffic analysis that is timely, efficient and relevant to keep our networks safe and secure.

Automation, Artificial Intelligence & Machine Learning

The ability to improve decision making about malware and to monitor and secure networks and devices from emerging threats.

Strategic Drivers

Australia needs to remain at the forefront of cyber security technology to anticipate and remain agile in the face of new and emerging threats. The strategic drivers include the need for research to support disruption – learning and understanding the inherent weaknesses of systems, the protection of critical infrastructure and systems of national significance, countering malicious cyber actors (state-based and criminals) and strengthening our nation's cyber resilience for all Australians. As our threats evolve – ever changing and more quickly, so must our responses and strategically focused research to allow us to deliver world-leading cyber security capability. Partnerships are essential to achieving this technological edge and sustaining the research pipelines that produce it.

Science and Technology Challenges

Through a process of consultation and analysis, four priority challenges were identified to be pursued for research and development.

1. Network and sensor

   Network and sensor technologies encompasses physical network infrastructure, network software and protocols, and new applications of network capability to new devices. Within this theme falls; the growing base of Internet of Things connected devices, wireless sensors, and technologies and techniques for network structure and operation. Cities in Australia are beginning the process of being transformed by the proliferation of Internet of Things devices and the implementation of technologies to track and manage service delivery. While this technology creates new opportunities for efficiency and convenience, it also gives rise to substantial security risks. Research that can inform and assess risks associated with devices and increase cyber resilience will enable the move to the smart city model in a secure manner.

   Cyber resilience is the measure by which an entity is capable of continuing to operate and deliver intended results during and after a cyber-attack. In its broadest sense, cyber resilience includes consideration of information security alongside business or organisation continuity. While cyber security centres on the prevention of system, network or data breach, cyber resilience responds to the effect of a given breach. Capabilities to promote security and continuity of next generation networking and sensor technologies will increase cyber resilience.

   Examples of science and technology research include:

   - Sensor technologies – Internet of Things
   - Edge Computing
   - 5G
   - IPV6; and
   - Software Defined Networking.

2. Data science

Data science in cyber security presents opportunities for improved decision making and intelligence gathering tools in areas such as digital forensics and network traffic analysis. As the available volume of data continues to increase so will the volume of malware, improved techniques and applications are needed to ensure analysis is timely, efficient, and relevant to keep our networks safe and secure.

Examples of science and technology research include:

- Modelling of complex human and technical systems
- Natural language processing
- Neural network analytical tools
- Digital forensic tools; and
- Biometrics.

3. Cryptography

Stakeholders have an ever-present and increasing need to assure the secrecy of the data they rely upon. However as data volume increases, current technologies require significant processing power to constantly encrypt and decrypt communications and stored data. Further, the security of these encryption technologies is at risk, particularly with the continued development of quantum computing technologies. While still future based, quantum computers will likely have the capacity to readily and frequently break most current encryption protocols. Such technologies as ubiquitous encryption, homomorphic encryption and blockchain are potential research solutions.

Examples of science and technology research include:

- Ubiquitous encryption
- Homomorphic encryption
- Quantum-safe encryption; and
- Blockchain.

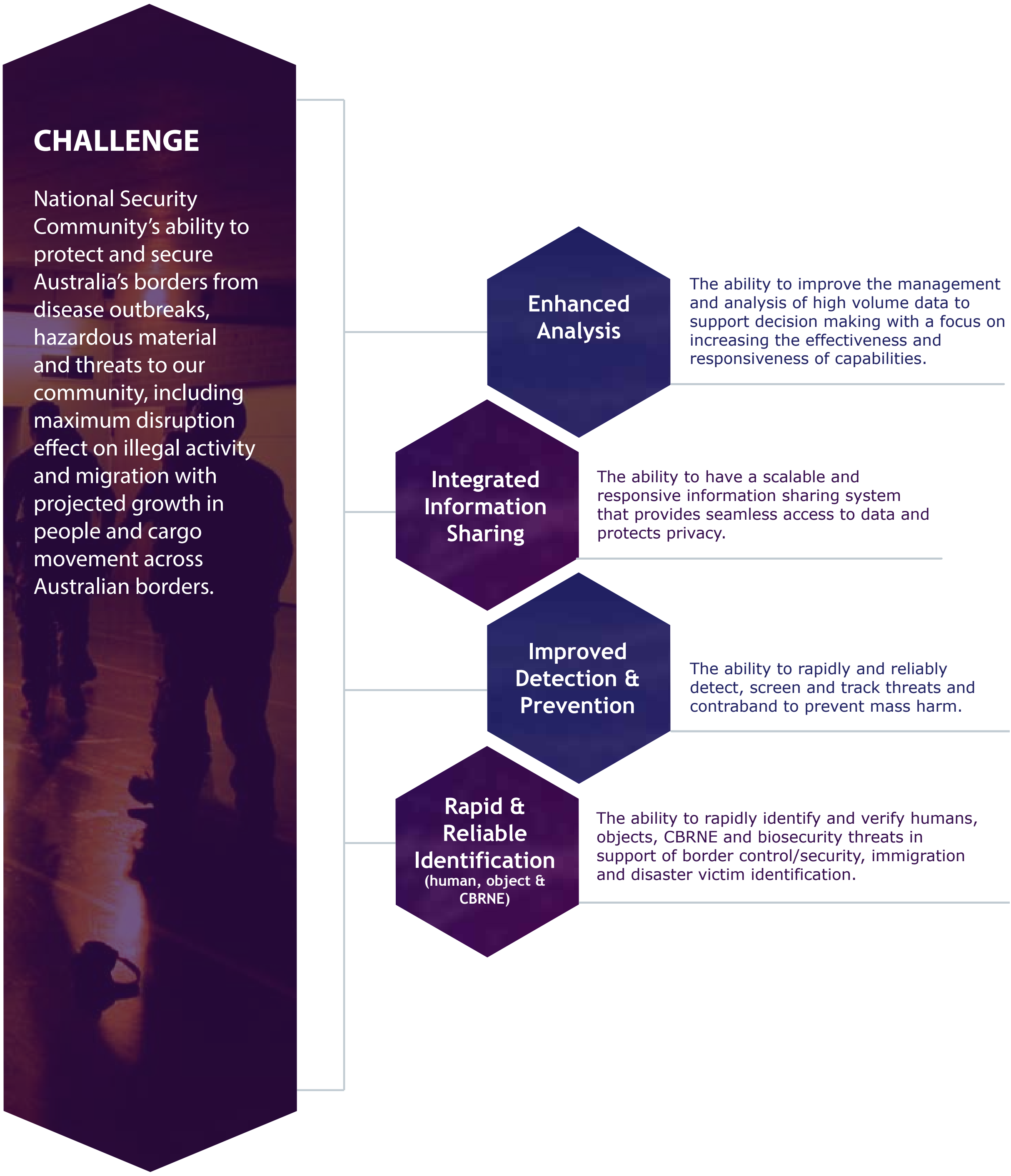
4. Auromation, artificial intelligence and machine learning

The application of AI and ML techniques can automate repetitive tasks usually performed by humans. AI and ML continue to learn when exposed to more data and applied to new use cases. Such recent improvements have seen AI and ML techniques becoming democratised: achievements and applications that five to ten years ago would have only been possible through research labs and extended doctoral investigation are now in the hands of the masses. These tools and techniques create challenges, like the emerging threat of deepfakes (AI generated lifelike videos and photographs) and evasive malware (able to detect its environment and institute behaviours to avoid detection), but also give rise to opportunities. AI and ML techniques have the capacity to be utilised to improve decision making, and to monitor and secure networks and devices.

Examples of science and technology research include:

- Prevention, detection and response
- Deep learning for network traffic and malware analysis; and
- Autonomous vehicles and robotics.

BORDER SECURITY AND IDENTITY MANAGEMENT



CHALLENGE

National Security Community's ability to protect and secure Australia's borders from disease outbreaks, hazardous material and threats to our community, including maximum disruption effect on illegal activity and migration with projected growth in people and cargo movement across Australian borders.

Enhanced Analysis

The ability to improve the management and analysis of high volume data to support decision making with a focus on increasing the effectiveness and responsiveness of capabilities.

Integrated Information Sharing

The ability to have a scalable and responsive information sharing system that provides seamless access to data and protects privacy.

Improved Detection & Prevention

The ability to rapidly and reliably detect, screen and track threats and contraband to prevent mass harm.

Rapid & Reliable Identification (human, object & CBRNE)

The ability to rapidly identify and verify humans, objects, CBRNE and biosecurity threats in support of border control/security, immigration and disaster victim identification.

Strategic Drivers

Preserving Australia's border integrity is a key challenge for the Australian Government. The projected growth in people and cargo movement across Australian borders is challenging Australia's ability to identify and assess risks and to conduct timely interventions. An efficient, safe and secure aviation and maritime systems are integral to Australia's social and economic prosperity. Managing the increased levels of planned and unplanned migration, refugee movement, and potential conflicts is a challenge for the government. Public trust and confidence in surveillance capabilities has come under increasing scrutiny, in particular the impact to privacy. These concerns are currently arising in the context of facial recognition technologies. In addition the globalisation of threats is of concern, particularly with the increase of digitisation across society where physical borders are not a deterrent. Investigating identity fraud on this platform can be challenging. Identity management is important in combatting serious and organised crime, and protecting Australians from identity-enabled cybercrime. As new operational challenges emerge, including biosecurity threats, the national security community needs to adapt to keep ahead of these threats to our safety and way of life.

Science and Technology Challenges

Through a process of consultation and analysis, four priority challenges were identified to be pursued for research and development.

1. Improved detection and prevention

   This theme reflects the need for developing rapid, reliable early detection and screening methods at the border for concealed contraband (e.g. drugs, weapons), threats such as CBRNE substances and biosecurity threats to prevent mass harm. The development of remote, stand-off and portable sensors and detectors to enable non-invasive screening can provide wide-ranging threat protection, while adapting security to the pace of life. This technology will improve security outcomes and the 'customer experience' and may provide a point of difference to operators.

   The national security community needs to be able to anticipate, identify and respond to an activity in real-time. This may include ongoing and sustained analyses of situation awareness in the physical world and how technological advancements can enable faster, more coordinated and targeted responses to events by operational response teams. Wide area surveillance technology for the detection, alert and tracking of small and large vessels to determine pattern of life will enable better situation awareness to determine potential intercept at sea to uphold border integrity.

   Examples of science and technology research include:

   - Remote sensor technology
   - Enhance human and technology detection performance;
   - Surveillance for detection of biosecurity threats; and
   - Surveillance for detection, alert and tracking of vessels.

2. Rapid and reliable identification (*human, object,* CBRNE)

The ability to rapidly identify and verify humans, objects, CBRNE and biosecurity threats is a challenge to national security. Science and technology research will focus on capabilities that support border control/security, disaster victim identification and immigration; in particular augmented biometrics to identify people suspected of terrorist activity and to prevent fraudulent identities, while ensuring privacy is protected. Fusing biometrics with biographical data and/or utilising multi-modal biometrics will improve identity confidence, whilst deterring potential identity fraud.

The combination of human and algorithm performance is critical to ensure reliable detection and identification of target entities. Accurately determining human identity is at the core of all immigration, visa and law enforcement decisions. Human social science and computational research will focus on methodologies, technologies and processes to increase the accuracy and reliability of algorithm and human decision making performance. This includes meeting scientific rigour to ensure public trust in biometric results is maintained.

Examples of science and technology research include:

- Biometric fusion with biographical data
- Behavioural biometrics
- Enhance algorithm and human performance
- Artificial Intelligence; and
- Mobile collection devices.

3. Integrated information sharing

An effective disruption approach requires cooperation on timely information sharing between the domestic national security community and trusted international partners to enable seamless access to data from which intelligence can be derived. To ensure effective information sharing, it is essential that the systems are scalable and responsive to national security needs and protect privacy. Science and technology solutions to improve technology performance, interpretation, interoperability and mitigate risks to privacy will ensure lawful and responsible sharing of Australia's information. This includes the ability to compare biometric data from different quality data sets and comply with domestic and international legislation, as well as the need for secure real-time linkages to internet facing capabilities.

Examples of science and technology research include:

- Data Fusion
- Single digital platform access
- Secure real time access; and
- Data protection, standards and privacy.

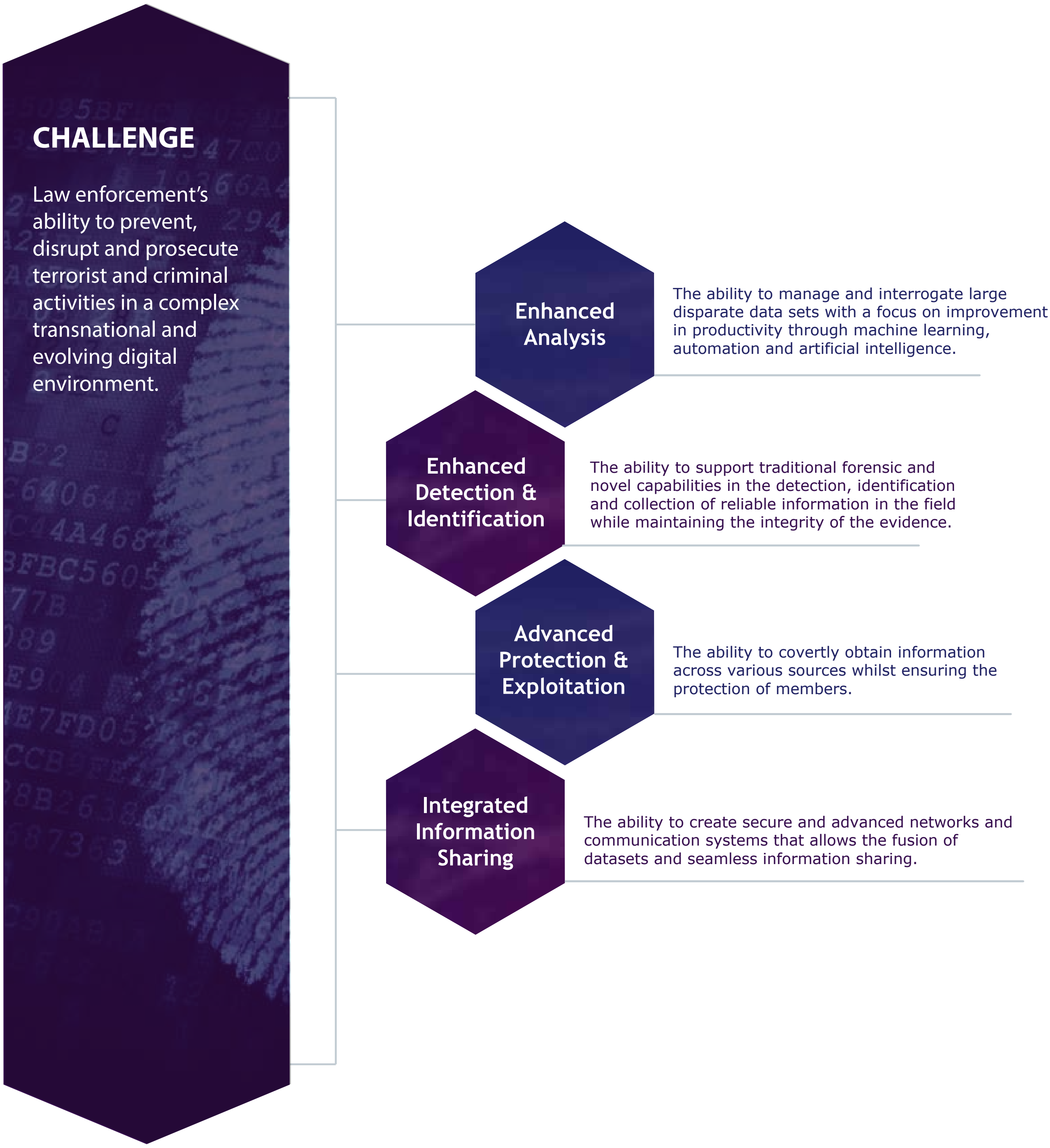
4. Enhanced analysis

This theme reflects the requirement to improve the management and analysis of high volume data to support decision making with a focus on increasing the effectiveness and responsiveness of capabilities/services. Machine learning and artificial intelligence has the potential to predict events and reduce processing time to maximise biometric matching and automated identity to improve risk and threat identification. Science and technology research will centre on fusing disparate information from different data sources to develop an understanding and automatically fuse, analyse and make sense of data and information at speed to enable evidence-based advice for security planning and operations.

Examples of science and technology research include:

- AI/ML
- Augmented intelligence
- Predictive analytics
- Behavioural analytics; and
- Risk analysis.

INVESTIGATIVE SUPPORT AND FORENSIC SCIENCE



CHALLENGE

Law enforcement's ability to prevent, disrupt and prosecute terrorist and criminal activities in a complex transnational and evolving digital environment.

Enhanced Analysis

The ability to manage and interrogate large disparate data sets with a focus on improvement in productivity through machine learning, automation and artificial intelligence.

Enhanced Detection & Identification

The ability to support traditional forensic and novel capabilities in the detection, identification and collection of reliable information in the field while maintaining the integrity of the evidence.

Advanced Protection & Exploitation

The ability to covertly obtain information across various sources whilst ensuring the protection of members.

Integrated Information Sharing

The ability to create secure and advanced networks and communication systems that allows the fusion of datasets and seamless information sharing.

Strategic Drivers

Forensic science continues to support both law enforcement and the broader national security community. It achieves this through the prevention and disruption of criminal activities and the prosecution of crimes. The Investigative Support and Forensic Science Program encompasses a wide span of traditional forensic disciplines, and continually seeks enhancement of these capabilities. Enrichment of capabilities includes seeking innovative solutions from industry and other sectors that can be applied through forensic frameworks to solve complex national security problems.

A unified approach across whole of government that supports interoperability and standardised information sharing (both domestically and internationally) will maximise our ability to ensure public safety. Australia needs to challenge its current systems, and harness advances in forensic science and technology to inform decision making, intelligence activities and the delivery of justice. The national security community must be capable of identifying physical threats including explosives, chemical, biological or radiological agents, drugs and items. An evolving digital environment challenges Australia's' ability to effectively utilise detection and collection methods, particularly for audio/visual that are fundamental to intelligence activities and the delivery of justice.

Science and Technology Challenges

Through a process of consultation and analysis, four priority themes were identified to be pursued for research and development.

1. Advanced protection and exploitation

   In the physical and digital world the collection of information has been hampered by the globalisation of the online world and national security threats as well as rapidly evolving technologies and the increased security-awareness of the criminal actors. Some capabilities find it increasingly difficult to perform their role effectively in a continuously changing complex environment. The national security community needs to adapt to the rapid changes in technology by researching avenues for new techniques and systems to enhance remote monitoring and information collection related to people, places and things. These can be addressed by enabling broader access across the community whilst also protecting national security interests.

   Examples of science and technology research include:

   - Deep analysis of systems
   - Biomarkers identification
   - Advanced methods and techniques for information collection
   - The extended and remote monitoring methods for people, places and things
   - Methods and tools to assess situations and environments; and
   - Counter measure development to ensure protection of members.

2. Enhanced detection and identification

This reflects the need to strive for scientific excellence in support of evidentiary requirements whilst also progressing technologically advanced solutions for information gathering and analytical activities. An example of this is the expanding field of DNA which is now extending into whole genome sequencing for non-human species. The national security community needs to drive emerging capabilities such as geospatial and geomatics examinations and support their admissible contribution to the judicial system through further research and consolidation of the science that underpins the integrity of evidence. Australia needs the ability to actively pursue advancing technologies to counter those utilised by criminal syndicates to evade authorities, particularly in relation to encryption and Internet of Things. Smaller and portable field equipment will allow for more timely identification and collection of information, as well as increased detection capabilities with a particular focus on the reliable reporting of CBRNE material in the field. The national security community also needs to adapt and explore the extension of current technologies to new opportunities.

Examples of science and technology research include:

- Detect, identify and collect information in the field quickly
- Stand off detection and collection of information
- Survivability and recovery of biometric data from extreme events (eg. bomb blast)
- Transforming lab based analysis to reliable and portable field instrumentation
- Encrypted device identification and analysis
- Forensic attribution and identification of the source of people, places and things
- Empirical studies related to novel capabilities i.e geospatial; and
- Advanced methods and techniques for the capture of audio and visual.

3. Enhanced analysis

The digital collection and analysis of data using enhanced computer processing will enable effective interrogation and assessment of multiple data sets to ensure rapid decision making. The adaptation of practices in non-related industries applied to investigative, intelligence and forensic processes require further refinement and application to the specific data sets utilised by national security organisations. The incorporation of Artificial Intelligence, Machine Learning and Data Science to existing investigative support and forensic processes will directly increase capacity, productivity and identify data fusion in a more predictive capacity.

Examples of science and technology research include:

- ML to advance pattern recognition
- Predictive analytics based on multiple data sets
- Exploitation of data sets rapidly
- Methods of translation for audio and visual
- Advanced biometric analysis; and
- The automation of current forensic processes.

4. Integrated information sharing

The globalisation of threats and the scale at which Australia responds to them has highlighted the requirement for interoperability between our people, processes and systems domestically, but also across our international partners who contribute to safeguarding Australia. A coherent approach to secure communication and systems infrastructure will enable greater resilience within capabilities to respond to threats or incidents, and achieve increased capacity and productivity. Assimilated systems, accessed through a single platform, enables more effective data fusion across whole of government and sharing opportunities which leads to timely decision making. This also aligns with the theme of enhanced analysis which can further leverage off integrated systems.

Examples of science and technology research include:

- Single Platform data access
- Secure communications in remote access areas; and
- The fusion of disparate data sets to obtain forensic intelligence.